

Appln. No. 09/896,163
Amdt. dated September 19, 2005
Reply to final Office Action of May 12, 2005

PATENT

REMARKS/ARGUMENTS

Claims 1-10 and 12-21 were pending. Claims 1-10 and 12-21 were variously rejected under 35 USC 103(a) in light of Yatsukawa in view of Baskey and in view of Chang or Arthan.

The undersigned accepts the Examiner's suggested title for the patent application.

I. THE PRESENT INVENTION

Embodiments of the present invention relate to secure computer network access.

As discussed previously, with embodiments of the present invention, a user does not need to have a hardware or software "token" to gain network access. Instead, the user only needs to have an authentic public/private key pair. In the embodiment illustrated in Figs. 4A-D, the user enters a correct password into a key wallet to retrieve their private key and digital certificate (steps 400-470).

In the various embodiments, the client then requests a one-time password from an external server, step 490. In response, the external server provides the one-time password, which is inactive back to the client, steps 500-530. Accordingly, if any one intercepts the one-time password at this stage, and attempts to gain access to the system, because the one-time password is inactive, the access will be denied. Further, because the one-time password is initially determined, and provided in the challenge, the one-time password should be inactive. Otherwise, a client who receives the challenge will be able to gain access to the network using the one-time password, even though she may be unauthorized.

Notice that before steps 500-530, the client does not have the one-time password. These embodiments allow the one-time password to be freely set, to be different for different users, and to be different for multiple user sessions, and the like. Additionally, these embodiments do not require the user to have any token hardware, to pre-register their client system, or to pre-register user data, as discussed above.

Appln. No. 09/896,163
Amdt. dated September 19, 2005
Reply to final Office Action of May 12, 2005

PATENT

Next, in various embodiments the client uses the received one-time password and digitally signs it with the private key to form a digital data packet (a digital signature), step 540. The digital signature and the user's digital certificate are then sent back to the external server, step 560. Accordingly, data from the external server is signed and then returned to the external server.

Subsequently, if the digital signature and digital certificate authenticate the user, the one-time password is activated, and the client may use the one-time password to access the protected computer network. Steps 570-690. In various embodiments, if the user is not authenticated and the client attempts to use the one-time password to access the network, the access will be denied. Accordingly, the one-time password in the challenge to the client should be inactive until the user is authenticated.

Certain limitations in the disclosed embodiments are recited in the claims. For example, among other limitations, claim 15, which was un-amended recites: means for forming a digital signature in response to the network password received from the verification server and to the private key; means for communicating the digital certificate and the digital signature to the authentication server; and means for receiving a challenge from a verification server via a first secure communications channel, the challenge comprising at least a network password that is inactive.

II. THE CITED REFERENCES

A. Yatsukawa

Yatsukawa relates to an authentication system where seed values Ds0 used to authenticate a user are initially synchronized.

In Yatsukawa, the client / user sets an initial "seed data" Ds0 for authentication purposes in the client and the server, Cols. 15, line 66 - Col. 16, line 12. From Ds0, Dn-1 are subsequently independently generated on a client and a server. In operation, Yatsukawa describes that the client logs into a server, col. 16, lines 46-52. Next, the server sends an authentication-data request, col. 16, lines 54-55. Then, the client generates authentication data D

Appln. No. 09/896,163
Amdt. dated September 19, 2005
Reply to final Office Action of May 12, 2005

PATENT

by enciphering the seed data Ds0 by the client private key K, and then D is sent back to the server, col. 16, lines 57-60. The server then decipheres the authentication data D using the client public key K to recover the client seed data. Col. 17, lines 1-14. Next, the server compares the recovered client seed data to the initial seed data previously provided by the user, Ds0. Col. 17, lines 14-17. As illustrated in Fig. 13, block S5, if the recovered client seed data matches Ds0, access is granted.

B. Chang

Chang relates to a token caching security system.

Chang states that one method of reducing remote access security risks is through the use of a "Smart card or Token card." Col. 2, lines 11-13. One such card is disclosed as "the SecurID card commercially available from Security Dynamics, Inc.," Col. 2, lines 13-14. Chang states that the function of the Token card is that it "generates a series of random one-time passwords (OTPs)." Col. 2, lines 15-16.

Chang describes that the Token card is used by the user. Specifically, Chang states:

To use the Token card, the user typically enters a series of digits and letters displayed on the token-card in the prompt window or inserts the card into a reader that is coupled to the Remote Node. Col. 2, lines 25-28. Emphasis added.

The series of digits and letters provided by the user is the one time password (OTP). This user-entered OTP is then compared to an OTP independently generated in a password server. Specifically, Chang states:

The password server internally generates OTPs in synch with the card. the OTP is then used to verify that the user is allowed to log into the network access server through the remote device ... by comparing the card password to the password server's password at a particular instant in time. Col. 2, lines 28-34. Emphasis added.

Appln. No. 09/896,163
Amdt. dated September 19, 2005
Reply to final Office Action of May 12, 2005

PATENT

As can be seen, in Chang, the OTP generated by the password server is not ever provided to the user. Instead, the user provides the OTP generated by the Token card to the password server.

Chang notes that use of Token cards by users to generate OTPs is burdensome. More specifically, Chang states:

However, a drawback with using OTPs is that additional connections ... are treated as separate connections. Thus, to establish a second session ... the user is required to reenter valid user identification information a second time. Because the OTP is only valid "once", the user must again use the token card to obtain another OTP that can be used to validate the second connection. Col. 2, lines 55-60.

In response, the invention in Chang appears to be a way to reduce having the user use the Token card to enter OTPs for each user session. Col. 3, lines 13-17.

In Chang, initially, the user uses a Token card to generate an OTP and then the user provides the OTP to a authenticating server. Specifically, Chang states:

The method comprises the steps of receiving a request to establish a session between the client and the first server, wherein the request includes identification information for authenticating a requesting user. Col. 3, lines 25-29. Emphasis added.

Chang also states that the identification information includes the OTP. Specifically:

One feature of this aspect is that the identification information includes a user name and a one-time password (OTP). col. 3, lines 35-37. Emphasis added.

In response to the user request, an authentication step is performed. If the user is authenticated, the identity information is cached. Specifically,

Appln. No. 09/896,163
Amdt. dated September 19, 2005
Reply to final Office Action of May 12, 2005

PATENT

determining, based on the identification information, whether the session between the client and the first server should be established, if the session between the client and the first server should be established, caching the identification information in memory; and establishing the session between the client and the first server. Col. 3, lines 29-34. Emphasis added.

Chang notes that a second server may be used to determine whether the session should be established. Specifically,

[T]he step of determining whether the session between the client and the first server should be established comprises the step of the first server communicating with a second server to determine whether the OTP is currently valid. Col. 3, lines 37-41.

Additionally, Chang notes that the second server checks whether the identification information is cached therein. Specifically,

[C]ommunicating with a second server to determine whether the OTP is currently valid further includes the steps of the second server determining whether the username and the OTP were previously cached in memory; and if the user-name and the OTP were not previously cached in memory, the second server communicating with a password server to determine whether the OTP is currently valid. Col. 3, lines 37-41.

If the identification information is cached, the cached identification information is checked to see if it is still valid. Specifically,

[C]ommunicating with a second server to determine whether the OTP is currently valid further comprises the step of the second server determining whether the username and the OTP were previously cached in memory; and if the user-name and the OTP were previously cached in memory, determining whether the username and the OTP are still valid. Col. 3, lines 52-58.

Appln. No. 09/896,163
 Amdt. dated September 19, 2005
 Reply to final Office Action of May 12, 2005

PATENT

This embodiment is repeated in the Detailed Description, on Col. 4, lines 31-67, etc. Importantly, on Col. 6, lines 42-47, Chang describes that in block 302 of Fig. 3A, the user provides a request to establish a session, and the request includes the username and OTP. In TABLE 1, Col. 8, lines 24-32, Chang gives an example, where the user "JOE" submits the request and enters a "username="JOE"," "CHAP password ="ABCD"," and "OTP = "1234" (from hand-held card)."

TABLE 1

Time	Action by user or client	Action by AAA server
15	-1	The database associated with AAA is configured to allow token caching for user JOE. User Identification Information for JOE is configured to expire based on session expiration and a cache time-out value of "60". A CHAP password of "ABCD" is used to validate the connection.
20		
25	0 user JOE submits a first request to establish a first session by supplying the NAS with the following information: username = "JOE" OTP = "1234" (from hand-held card) CHAP = "ABCD"	In this example, the AAA server currently has no cached information for user JOE. Thus, the AAA server communicates with a token server to verify the OTP "1234". The AAA server also validates the CHAP password "ABCD".
30	1 User JOE authenticates successfully.	Authentication is successful. The AAA server stores in its cache the username "JOE" and the OTP "1234". The AAA server also generates and stores session information.
35		

Next, on Col. 6, lines 48-50, Chang describes that in block 304 of Fig. 3A, the AAA server determines whether the session should be established based on the "user identification information" received from the user. In TABLE 1, Col. 8, lines 24-31, Chang gives an example, where the AAA server communicated with a token server to verify OTP "1234" and validates CHAP password "ABCD."

C. Baskey

Baskey was previously discussed as relating to an SSL proxy server, and being silent regarding an authentication protocol.

Appln. No. 09/896,163
Amdt, dated September 19, 2005
Reply to final Office Action of May 12, 2005

PATENT

III. THE CITED REFERENCES DISTINGUISHED

A. Claim 15

The elements of Claim 15 are not disclosed, suggested, or taught by Yatsukawa in view of Baskey or Chang. More specifically the cited references fail to disclose means for receiving a challenge from a verification server via a first secure communications channel, the challenge comprising at least a network password that is inactive. The undersigned points out that the underlined claim language was not entered by amendment, but was a limitation found in claim 15 of the original patent application, and was a limitation found in claim 15 the first office action response. Accordingly, this limitation is not new.

As discussed above, Yatsukawa is a form of "token-based" authentication where the client determines the authentication-data inspection data. Importantly, in Yatsukawa, the challenge from the verification server to the client system does not include "a network password that is inactive," as is recited above. In Yatsukawa, the client must already have seed data in memory, and must be presynchronized with the server.

Additionally, Baskey is silent as to this limitation, as Baskey simply relates to SSL connections.

As discussed above, the user in Chang uses a Token card in her possession to obtain a one time password (OTP). A network password is not received from the verification server. Further, in Chang, the OTP that is independently determined in the authentication server is not initially inactive. As illustrated above, when the OTP from the Token card and the user simply matches the OTP independently determined in the AAA server, the user session is initiated. The password determined in the server is not inactive and then activated in Chang. Instead, once determined, the OTP is always active. Similarly, in Yatsukawa, Ds0 determined in the server is not inactive and then activated, but, once determined, is always active.

The references also fail to disclose means for forming a digital signature in response to the network password received from the verification server and to the private key,

Appln. No. 09/896,163
Amdt. dated September 19, 2005
Reply to final Office Action of May 12, 2005

PATENT

and means for communicating the digital certificate and the digital signature to the authentication server.

This limitation is totally missing from Chang. Additionally, Yatsukawa, at best describes digitally signing seed data already present on the client. In contrast, the digital signature is claimed to be determined in response to the network password that was received from the verification server.

Accordingly, because these cited references fail to disclose at least the above recited limitations, claim 15 is patentable.

B. Remaining Claims

Claims 1 and 8, are believed to be allowable for at least the same reasons as those given above for claim 15, and more particularly, for the specific limitations they recite. The Examiner is directed to examine the exact wording of each of these claims.

Claims 2-7, which depend from claim 1 are believed to be allowable for at least the same reasons given above, and more particularly, for the specific limitations they recite, thus the pending rejections are traversed. The Examiner is directed to examine the exact wording of each of these claims.

Claims 9-10 and 12-13 which depend from claim 8 are believed to be allowable for at least the same reasons given above, and more particularly, for the specific limitations they recite, thus the pending rejections are traversed. The Examiner is directed to examine the exact wording of each of these claims.

Claims 16-20, which depend from claim 15 are believed to be allowable for at least the same reasons given above, and more particularly, for the specific limitations they recite. The Examiner is directed to examine the exact wording of each of these claims.

Appln. No. 09/896,163
Amtd. dated September 19, 2005
Reply to final Office Action of May 12, 2005

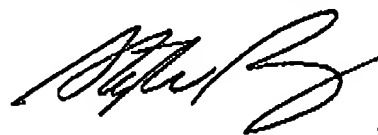
PATENT

CONCLUSION

In view of the foregoing, Applicants believe all claims now pending in this Application are in condition for allowance and an action to that end is respectfully requested.

If the Examiner believes a telephone conference would expedite prosecution of this application, please telephone the undersigned at 650-326-2400.

Respectfully submitted,



Stephen Y. Pang
Reg. No. 38,575

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, Eighth Floor
San Francisco, California 94111-3834
Tel: (650) 326-2400
Fax: (650) 326-2422
SYP:deh
60512811 v1